Amendments to the Claims:

1. (Currently amended) A method for sending secure messages in a broadcast network comprising the steps of:

encrypting data with a key;

hashing said key;

combining said encrypted data and said hashed key in a broadcast message that is structured so as to be capable of being decrypted by each of a plurality of receiving nodes; and

transmitting said broadcast message to ~~a~~ the plurality of receiving nodes.

2. (Currently amended) The method of claim 1 wherein the key is one of a plurality of different keys and said steps of combining and transmitting comprises:

combining said encrypted data with each one of said plurality of different keys in a plurality of broadcast messages; and

transmitting one of the plurality of broadcast messages to a subset of said plurality of receiving nodes.

3. (Currently amended) The method of claim 2 wherein each one of said plurality of different keys ~~are~~ is associated with a respective category of messages.

4. (Currently amended) A method for decrypting a message received over a broadcast network comprising the steps of:

receiving data comprising an encrypted message and a hashed key at a node in said broadcast network, wherein said node comprises means for storing data;

parsing said data to derive said encrypted message and said hashed key;

comparing said received hashed key with a plurality of keys ~~stored~~ that are prestored in said means for storing data in said node and to select a key having a hash matching said received hashed key; and

decrypting said encrypted message with said matching key if a match was found.

5. (Currently amended) The method of claim 4 further comprising the step of requesting a key from a network entity if no prestored key is found to have a hash that matches said received hashed key.

6. (Currently amended) In a communications network having a plurality of network entities, a first one of the network entities comprising:

a means encrypting data with a key;

a means for hashing said key;

a means for combining said encrypted data and said key in a broadcast message that is structured so as to be capable of being decrypted by each of a plurality of receiving nodes; and

a means for transmitting said broadcast message to ~~a~~ the plurality of receiving nodes.

7. (Original) The network entity of claim 5 further comprising a means for distributing hashed keys.

8. (Currently amended) A computer-readable memory for directing a computer to function in a particular manner when used by the computer, comprising:

a first portion to direct the computer to encrypt data with a key;

a second portion to direct computer to hash said key;

a third portion to direct computer to combine said encrypted data with said hashed key in a broadcast message that is structured so as to be capable of being decrypted by each of a plurality of receiving nodes; and

a fourth portion to direct computer to provide multiple transmissions of said message.

9. (Currently amended) A computer-readable memory for directing a computer to function in a particular manner when used by the computer, comprising:

a first portion to direct the computer to receive data comprising an encrypted message and a hashed key;

a second portion to direct computer to parse said data;

a third portion to direct computer to compare said received hashed key with a plurality of keys and to select a key having a hash matching said received hashed key; and a fourth portion to direct computer to decrypt said encrypted message with said matching key if a match was found and send request for key to a network entity if no matching key was found.

10. (Currently amended) A computer data signal embodied in a carrier wave, comprising an encrypted message, a hashed key and instructions for:

parsing said data to derive said encrypted message and said hashed key;

comparing said received hashed key with a plurality of keys that are prestored by a receiving ~~stored in said means for storing data in said~~ node to select a key having a hash matching said received hashed key; and

decrypting said encrypted message with said matching key if a match was found and sending request for key to a network entity if no matching key was found.

11. (Currently amended) A computer program product that enables a network entity to distribute secure content in a network comprising:

computer readable code that instructs computer to:

encrypt data with a key;

hash said key;

combine said encrypted data and said hashed key in a broadcast message that is structured so as to be capable of being decrypted by each of a plurality of receiving nodes;

transmit multiple transmissions of said broadcast message;

and

a tangible medium that stores the computer readable code.

12. (Original) The computer product of claim 11 wherein the tangible medium is selected from a group consisting of hard-disk, CD-ROM, DVD, floppy disk, flash memory and the like.

13. (New) A computer-readable memory of claim 9 wherein said third portion is adapted to compare said received hashed key with a plurality of keys that have been prestored by the computer.

14. (New) A method of claim 4 wherein receiving data comprises receiving the same data comprising an encrypted message and a hashed key at each of a plurality of nodes in said broadcast network, and wherein said parsing, comparing and decrypting steps are performed at each of the plurality of nodes in said broadcast network.

15. (New) A method of claim 1 wherein combining said encrypted data and said hashed key comprising combining said encrypted data and said hashed key to create the broadcast message that is independent of any representation of a key that would be specific to and only capable of being decrypted by a single receiving node.

16. (New) A network entity of claim 6 wherein said means for combining said encrypted data and said hashed key is also capable of combining said encrypted data and said hashed key to create the broadcast message that is independent of any representation of a key that would be specific to and only capable of being decrypted by a single receiving node.

17. (New) A computer-readable memory of claim 8 wherein said third portion is also capable of directing the computer to combine said encrypted data and said hashed key to create the broadcast message that is independent of any representation of a key that would be specific to and only capable of being decrypted by a single receiving node.

18. (New) A computer program product of claim 11 wherein said computer readable code is also capable of instructing the computer to combine said encrypted data and said hashed key to create the broadcast message that is independent of any representation of a key that would be specific to and only capable of being decrypted by a single receiving node.